PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: **John M. Hammer et al.**	)	
	)	Art Unit: **2135**
Application No.: **09/685,285**	)	
	)	Examiner: **Leynna A. Ha**
Filed: **October 10, 2000**	)	
	)	Confirmation No.: **4449**
For: **Method and System for Creating a Record for One or More Computer Security Incidents**	)	Attorney Docket No. **05456.105008**

APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

July 6, 2007

Sir:

Further to the Notice of Appeal filed on June 4, 2007 in the above referenced application, Appellants hereby submit this brief under 37 C.F.R. § 1.191 to appeal the Examiner's rejection of this application, as reported in the Final Office Action mailed on March 20, 2007.

I hereby certify that this correspondence is being electronically transmitted to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450, on July 6, 2007.

/SPW/
Steven P. Wigmore, Reg. No. 40,447

Table of Contents

Real Party in Interest 3
Related Appeals and Interferences 4
Status of Claims 5
Status of Amendments 6
Summary of Claimed Subject Matter 7
Grounds of Rejection to be Reviewed on Appeal 11
Argument 12
Conclusion 23
APPENDIX 1 - Claims Appendix 24
APPENDIX 2 - Evidence Appendix 38
APPENDIX 3 - Related Proceedings Appendix 39

Real Party in Interest

The real party in interest is IBM Internet Security Systems, formerly operating as Internet Security Systems, Inc., the assignee of record. IBM Internet Security Systems is a wholly owned subsidiary of International Business Machines (IBM), Inc.

Related Appeals and Interferences

None.

Status of Claims

Claims 1-9 and 11-65 stand finally rejected and are on appeal. Claim 10 has previously been canceled and is not on appeal.

Status of Amendments

No additional amendments have been filed subsequent to the final rejection mailed on March 20, 2007.

Summary of Claimed Subject Matter

In general, the invention disclosed by the present application defines a method and system for creating a record of investigations and responses to one or more security incidents that may occur on or within a computer system. (page 4, lines 22-24). Specifically, a computer security management system produces a security record of information related to the tracking of suspicious computer activity or actual computer security threats, such as denial of service attacks or other similar compromises to computers or computer networks. (page 4, lines 24-27). The security record can include, but is not limited to, dates and times of computer security incidents, computer security threat procedure information, such as a name for a particular security incident, and executed response steps taken by a user. (page 4, lines 27-29 and page 5, lines 8-11). The security record can be designed as a running log that saves or records all observable activity of a computer incident source as well as the activity of the security team responding to the computer incident source. (page 4, lines 29-31).

The computer security management system also can classify computer security incidents according to selective attributes. (page 5, lines 24-26). In some exemplary embodiments, this security record can be permanent (page 5, lines 13-15; see claims 42, 51, and 56). By making this security record permanent, such a record can be admitted as forensic evidence in a court of law (page 5, lines 13-15).

The computer security management system can generate displays for organizing and collecting information about a computer security incident. (page 6, lines 10-12). For example, the computer security management system can provide a listing of investigation procedures and response procedures. (page 6, lines 12-14).

Each procedure can include one or more steps that can be displayed as text listed in a sequential order. (page 6, lines 15-16). After each step of a selected computer security threat procedure is executed, the computer security management system can save or record the step taken, the results produced by the step and a corresponding date or time stamp or both to a local database. (page 7, lines 7-9).

In certain additional exemplary embodiments, the computer security management system can locate an appropriate computer to execute steps of a procedure by accessing a table containing predetermined data. (page 7, lines 23-25). For example, to execute certain steps in response procedures that may include activity or behavior that is restricted in a computer

network, it may be necessary to find a computer located close to the perimeter or outer regions of the network to perform such restricted activities or behaviors. (page 7, lines 25-28). In other words, in some response scenarios, it may be necessary to locate computers in a network that are not restricted to a limited number of "friendly" commands or operations. (page 7, lines 28-30).

Independent Claim 1 is directed to a method for automatically creating a record for one or more computer security incidents and reactions thereto. The method of Claim 1 includes the following steps: (1) recording computer security incident information with at least one of a date and time stamp, the computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat (page 4, line 22 to page 5, line 11; page 22, line 6 to page 25, line 25; page 26, lines 14-16; page 43, lines 21-24); (2) classifying the computer security incident information (page 6, lines 12-14, page 20, lines 19-22; page 44, lines 1-12); (3) automatically suggesting one or more computer security threat procedures based on a classification of the computer security incident information (page 6, lines 12-14, page 20, lines 19-22; page 44, lines 1-12); (4) displaying the one or more suggested computer security threat procedures, each computer security threat procedure comprising one or more steps for one of investigating and responding to the computer security incident information (page 6, lines 7-23; page 44, lines 13-16); (5) receiving a selection of a suggested computer security threat procedure from a user, the selection comprising one or more steps of the selected computer security threat procedure (page 6, lines 15-17; page 28, line 24 to page 29, line 4; page 46, lines 18-21); (6) executing the selected one or more steps of the computer security threat procedure (page 6, lines 15-17; page 29, lines 3-21; page 46, lines 22-25); (7) in response to executing the one or more steps of the selected computer security threat procedure, recording executed computer security threat procedure information and results of the executed one or more steps of the computer security threat procedure with at least one of a date and time stamp (page 7, lines 7-9; page 46, lines 25-27); and (8) outputting a record comprising the computer security incident information, executed computer security threat procedure information, results of one or more steps of the executed computer security threat procedure, an identity of the user who selected the computer security threat procedure, and at least one of a corresponding date stamp and time stamp (page 7, lines 9-11; page 30 line 31 to page 31, line 2).

Independent Claim 42 is directed to a method for organizing and recording reactions to

one or more computer security incidents. The method of Claim 42 includes the following steps: (1) classifying the computer security incident information (page 6, lines 12-14, page 20, lines 19-22; page 44, lines 1-12); (2) automatically suggesting one or more computer security threat investigation procedures based on a classification of the computer security incident information (page 6, lines 12-14, page 20, lines 19-22; page 44, lines 1-12); (3) displaying the one or more computer security threat investigation procedures for investigating one of suspicious computer activity that occur prior to a computer security threat and an actual computer security threat (page 6, lines 7-23; page 44, lines 13-16); (4) displaying one or more computer security threat response procedures for responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat (page 6, lines 7-23; page 46, lines 11-18); (5) in response to a selection of a computer security threat investigation procedure, displaying one or more corresponding investigation steps; (6) in response to a selection of a computer security threat response procedure, displaying one or more corresponding response steps (page 6, lines 15-16; page 28, line 24 to page 29, line 4; page 46, lines 18-21); (7) receiving a selection of one or more investigation steps and one or more corresponding response steps (page 6, lines 15-17; page 29, lines 3-5; page 46, lines 11-21); (8) storing a permanent record comprising computer security incident information, executed investigation step and result information, executed response step and result information, and corresponding date and time stamps (page 5, lines 13-15; page 7, lines 7-9; page 46, lines 25-27).

Independent Claim 51 is directed to a method for selecting a computer that is strategically located relative to a source of a computer security incident. The method of Claim 51 includes the following steps: (1) accessing a table comprising computer locations, Internet address ranges associated with the computer locations, and computer security threat procedure associated with the computer locations, the computer security threat procedure comprising one or more steps for one of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat, the computer locations identifying devices that are able to perform the computer security threat procedure (page 6, lines 13-21; page 7, lines 23-25); (2) comparing a computer security threat procedure to be executed and a target Internet address with computer locations and Internet address ranges listed in the table (page 47, lines

14-23); (3) determining if a match exists between an Internet address of a computer security incident and the Internet address ranges listed in the table (page 47, lines 14-30); (4) automatically selecting a computer to execute the computer security threat procedure based upon the matching step, wherein the computer has a location and is capable of interacting with the Internet address of the computer security incident (page 47, lines 14-30); and (5) storing a permanent record comprising the executed computer security threat procedure and result information, and corresponding date and time stamps (page 5, lines 13-15; page 7, lines 7-9; page 46, lines 25-27).

Independent Claim 56 is directed to a method for generating a permanent record of one of more computer security incidents and reactions thereto. The method of Claim 56 includes the following steps: (1) receiving computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat (page 4, line 22 to page 5, line 11; page 22, line 6 to page 25, line 25; page 26, lines 14-16; page 43, lines 21-24); (2) classifying the computer security incident information (page 6, lines 12-14, page 20, lines 19-22; page 44, lines 1-12); (3) displaying one or more tools for one of investigating and responding to computer security incident information (page 6, lines 7-23; page 29, lines 3-4; page 44, lines 13-16); (4) automatically suggesting one or more tools based on a classification of the computer security incident information (page 6, lines 12-14, page 20, lines 19-22; page 44, lines 1-12); (5) receiving a selection of a suggested tool (page 6, lines 15-17; page 28, line 24 to page 29, line 4; page 46, lines 18-21); (6) in response to a selection of a tool, forwarding data for execution of the tool (page 47, lines 23-25); and (7) forwarding data for storing a permanent record comprising computer security incident information, executed tool information, and corresponding date and time stamps (page 5, lines 13-15; page 7, lines 7-9; page 46, lines 25-27).

[GO TO NEXT PAGE]

Grounds of Rejection to be Reviewed on Appeal

The following issue is presented on appeal:

Whether Claims 1-9 and 11-65 are unpatentable under 35 U.S.C. § 103(a) over U.S. Patent Nos. 6,298,445 to Shostack, et al. ("*Shostack*"), 6,453,345 to Trcka ("*Trcka*"), and 6,070,190 to Reps et ail. ("*Reps*").

Argument

Claim Rejections under 35 U.S.C. § 103(a)

The U.S. Patent and Trademark Office has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. In re Warner et al., 379 F.2d 1011, 154 U.S.P.Q. 173, 177 (C.C.P.A. 1967), In re Fine, 837 F.2d 1071, 1074, 5 U.S.P.Q.2d 1596, 1598-99 (Fed. Cir. 1988). To establish a *prima facie* case of obviousness, three basic criteria must be met. First, the prior art reference (or references when combined) must teach or suggest all the claim limitations. Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference(s) or to combine reference teachings. Finally, there must be a reasonable expectation of success. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on the Appellant's disclosure. In re Vaeck, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991).

Independent Claim 1

In the Office Action dated March 20, 2007, the Examiner rejected independent Claim 1 as allegedly being obvious in view of *Shostack* and *Trcka*. Appellant respectfully traverses this rejection. In particular, Appellant respectfully submits that the Examiner has not established a *prima facie* case of obviousness with respect to independent Claim 1 because the cited documents, including *Shostack* and *Trcka*, fail to teach or suggest at least the combination of the features of: (1) recording computer security incident information with at least one of a date and time stamp, the computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat; (2) classifying the computer security incident information; (3) automatically suggesting one or more computer security threat procedures based on a classification of the computer security incident information; (4) displaying the one or more suggested computer security threat procedures, each computer security threat procedure comprising one or more steps for one of investigating and responding to the computer security incident information; (5) receiving a selection of a suggested computer security threat

procedure from a user, the selection comprising one or more steps of the selected computer security threat procedure; (6) executing the selected one or more steps of the computer security threat procedure; (7) in response to executing the one or more steps of the selected procedure, recording executed computer security threat procedure information and results of the executed one or more steps of the computer security threat procedure with at least one of a date and time stamp; and (8) storing a record comprising the computer security incident information, executed computer security threat procedure information, results of one or more steps of the executed computer security threat procedure, an identity of the user who selected the computer security threat procedure, and at least one of a corresponding date stamp and time stamp.

Shostack

Shostack is directed to a system for automatically providing enhancements to computer security software. (See Abstract). The enhancements include updated information regarding security vulnerabilities. The system receives an enhancement from a network and integrates the enhancement into the computer security software. Before the integration, the system performs a computer check to determine the integrity and the authenticity of the enhancement. The computer check can use cryptographic techniques such as digital signatures and Pretty Good Privacy (PGP) encryption. (See column 2, lines 30-48).

With reference to Figure 5 of *Shostack*, reproduced below for reference, the system 160 includes a database 92 of security vulnerabilities and various modules. A first module 74 accesses the database 92 and assesses security vulnerabilities of an operating system of a computer. A second module 76 accesses the database and assesses security vulnerabilities of a computer network that includes the computer. A third module 78 accesses the database 92 and assesses security vulnerabilities in passwords used to access the computer or the network. A fourth module 88 accesses the database 92 and assesses security vulnerabilities of a remote computer connected to the network. A fifth module 90 receives an update to the database 92 and updates the database 92. A sixth module is a communications module that allows communication between the integrated security system 160 and a similar system. (See column 11, line 61 to column 12, line 14).

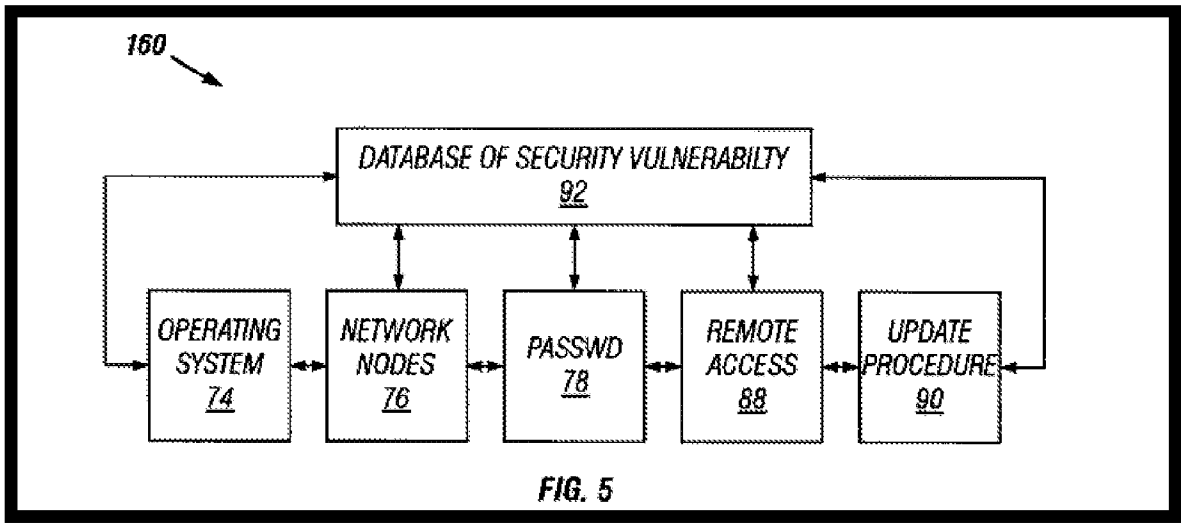

FIG. 5

Shostack explains that the aforementioned and above illustrated modules 74, 76, 78, 88, 90 of the integrated system 160 are represented by corresponding symbols on a graphical user interface (GUI) screen 70, as illustrated in Figure 6 of *Shostack*, reproduced below.

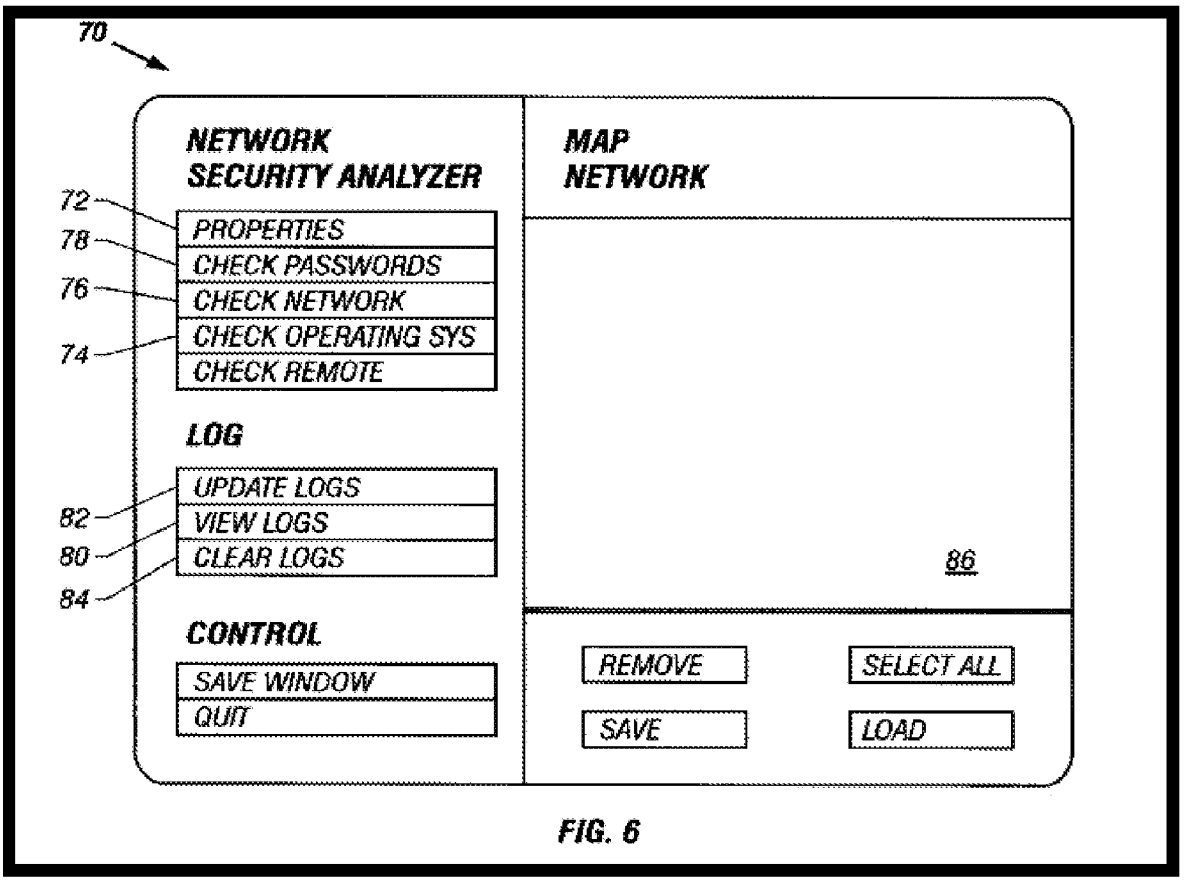

FIG. 6

Shostack explains that the GUI 70 provides a reporting mechanism. Specifically, the GUI 70 includes several means for reporting various network transactions. The GUI 70 includes a log view 80 that can allow a user to view a text version of an update process or log information on a storage device, a log update 82 that generates a report of all security vulnerabilities on the network 20, and a log clear function 84 that allows a user to erase the log.

In the Office Action dated March 20, 2007, the Examiner cited the GUI 70 of Figure 6 of *Shostack* as allegedly teaching the features of (1) displaying one or more suggested computer security threat procedures, each computer security threat procedure comprising one or more steps for one of investigating and responding to the computer security incident information; and (2) receiving a selection of a suggested computer security threat procedure, the selection comprising one or more steps of the selected computer security threat procedure. Appellant respectfully disagrees with this interpretation of *Shostack*. In particular, Appellant respectfully submits the GUI 70 of *Shostack* does not display one or more procedures comprising one or more steps or provide for the reception of a selection of one or more procedures comprising one or more steps.

For responding to security vulnerabilities, *Shostack* provides that "The update processor 54 also includes solutions for repairing the newly discovered vulnerabilities. The update processor 54 may automatically implement the suggested repairs of the system vulnerabilities and may send a message that the update is completed (Step 122)." (Column 11, lines 50-54). Therefore, in the system of *Shostack*, after a software enhancement is received, the suggested repairs of the system vulnerabilities are implemented without allowing for the display of one or more suggested computer security threat procedures or the selection of a suggested computer security threat procedure, the selection comprising one or more steps of the selected computer security threat procedure.

The Examiner further relies upon *Shostack* to provide an alleged teaching of storing a record comprising the computer security incident information, executed computer security threat procedure information, results of one or more steps of the executed computer security threat procedure, and an identity of a user who selected the computer security threat procedure. However, *Shostack* does not provide a teaching of the storage of this type of information. *Shostack* merely provides for the storage of the software enhancement that is received and a log of the software enhancement update. (See e.g., column 11, line 41; column 13, line 17).

In the Office Action dated March 20, 2007, the Examiner admitted that *Shostack* does not

teach the claimed features of a date and time stamp and receiving a selection of a suggested computer threat procedure. As discussed below, the Examiner cited *Trcka* as allegedly disclosing these features.

Therefore, Appellant submits that *Shostack* does not anticipate or render obvious independent Claim 1.

Trcka

Appellant respectfully submits that *Trcka* fails to correct the deficiencies of *Shostack*. In the Office Action dated March 20, 2007, the Examiner cited *Trcka* only for allegedly teaching a date and time stamp and receiving a selection of a suggested computer threat procedure. Even assuming for the sake of argument that *Trcka* teaches a date and time stamp and receiving a selection of a suggested computer threat procedure, Appellant respectfully submits that *Trcka* fails to teach or suggest at least the claimed features discussed above with reference to *Shostack*.

Therefore, Appellant submits that the cited documents, including *Shostack* and *Trcka*, either alone or in combination, do not anticipate or render obvious independent Claim 1. Accordingly, reconsideration and withdrawal of the rejection of Claim 1 are respectfully requested.

Independent Claim 42

In the Office Action dated March 20, 2007, the Examiner rejected independent Claim 42 as allegedly being obvious in view of *Shostack* and *Trcka*. Appellant respectfully traverses this rejection. In particular, Appellant respectfully submits that the Examiner has not established a *prima facie* case of obviousness with respect to independent Claim 42 because the cited documents, including *Shostack* and *Trcka*, fail to teach or suggest at least the combination of the features of: (1) classifying the computer security incident information; (2) automatically suggesting one or more computer security threat investigation procedures based on a classification of the computer security incident information; (3) displaying the one or more computer security threat investigation procedures for investigating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat; (4) displaying one or more computer security threat response procedures for responding to one of suspicious computer

activity comprising on or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat; (5) in response to a selection of a computer security investigation procedure, displaying one or more corresponding investigation steps; (6) in response to a selection of a computer security response procedure, displaying one or more corresponding response steps; (7) receiving a selection of one or more investigation steps and one or more corresponding response steps; and (8) storing a permanent record comprising computer security incident information, executed investigation step and result information, executed response step and result information, and corresponding date and time stamps.

In the Office Action dated March 20, 2007, the Examiner admitted that *Shostack* does not teach the claimed features of a date and time stamp and receiving a selection of a suggested computer threat procedure. Therefore, Appellant submits that *Shostack* does not anticipate or render obvious independent Claim 42. Applicant further submits that *Shostack* and *Trcka*, either alone or in combination, do not anticipate or render obvious independent Claim 42. As noted above with respect to independent Claim 1, neither *Shostack* nor *Trcka* disclose, teach, or suggest at least the features of (1) displaying one or more computer security threat investigation procedures and response procedures; and (2) receiving a selection of a computer security threat investigation procedure. Nor do *Shostack* or *Trcka* disclose, teach, or suggest the corresponding step of storing a permanent record comprising computer security incident information, executed investigation step and result information, executed response step and result information, and corresponding date and time stamps.

Therefore, Appellant submits that the cited documents, including *Shostack* and *Trcka*, either alone or in combination, do not anticipate or render obvious independent Claim 42. Accordingly, reconsideration and withdrawal of the rejection of Claim 42 are respectfully requested.

Independent Claim 51

In the Office Action dated March 20, 2007, the Examiner rejected independent Claim 51 as allegedly being obvious in view of *Shostack* and *Reps*. Appellant respectfully traverses this rejection. In particular, Appellant respectfully submits that the Examiner has not established a *prima facie* case of obviousness with respect to independent Claim 51 because the cited documents, including *Shostack* and *Reps*, fail to teach or suggest at least the combination of the

features of: (1) accessing a table comprising computer locations, Internet address ranges associated with the computer locations, and computer security threat procedure associated with the computer locations, (2) the computer security threat procedure comprising one or more steps for one of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat, (3) the computer locations identifying devices that are able to perform computer security threat procedure associated with the computer security step information; (4) comparing a computer security threat procedure to be executed and a target Internet address with computer locations and Internet address ranges listed in the table; (5) determining if a match exists between an Internet address of a computer security incident and the Internet address ranges listed in the table; (6) automatically selecting a computer to execute the computer security threat procedure based upon the matching step, wherein the computer has a location and is capable of interacting with the Internet address of the computer security incident; and (7) storing a permanent record comprising the executed computer security threat procedure and result information, and corresponding date and time stamps

Reps

Reps describes technology that is in the field of network system service, and particularly to an end-user based application availability and response monitoring and alerting system. The technology described by *Reps* enables the monitoring of availability of response time or other desired performance metrics of an application program from the perspective of an end-user utilizing an application program over a distributed computing network. (See column 1, lines 24-31.)

With reference to Figure 2 of *Reps*, reproduced below, *Reps* explains that a server computer 202 having an application program 203 provides application services to a client computer system 106 in which the client computer system 106 records information related to the performance of the services of the application program 203 via an application probe software 201 residing on the client computer system 1-6. (See column 5, lines 17-22).

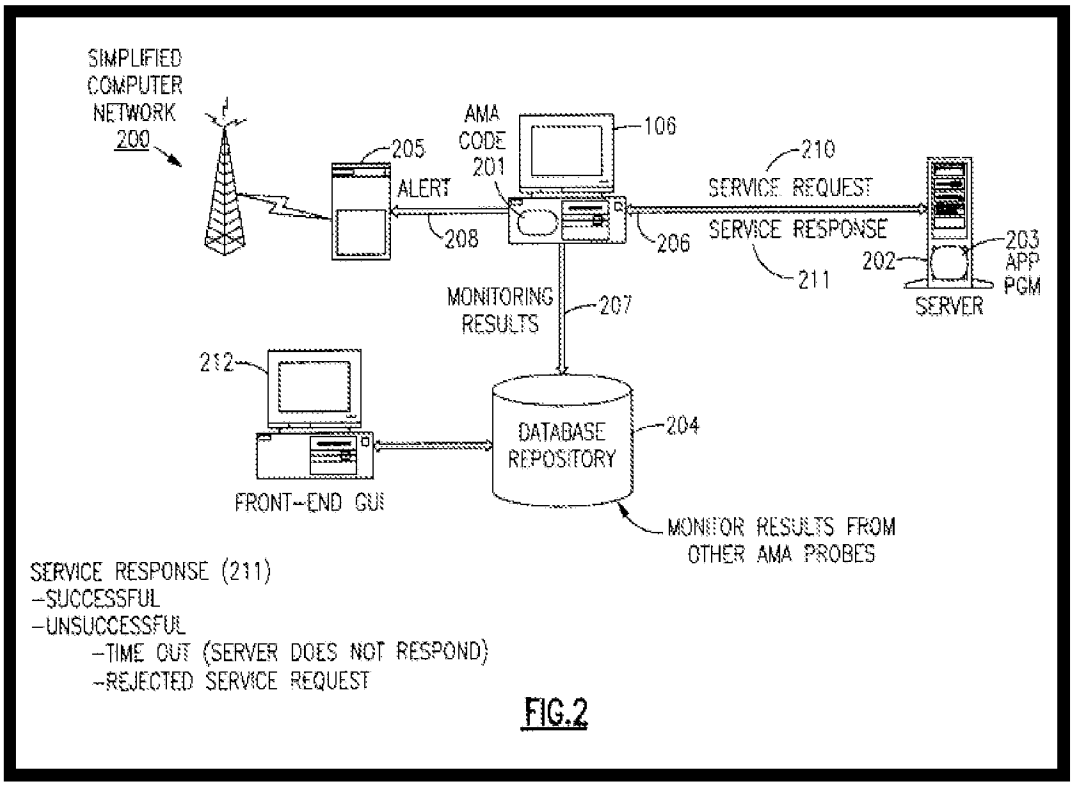

FIG.2

Specifically, as illustrated in Figure 2 above, an application monitoring alerting (AMA) probe 201 can establish a session with a server computer 202 by requesting the services of an application program 203 operating on the server computer 202 through a service request 210. The server computer's application program 203 provides a service response 211 over a network link 206 back to the requesting AMA probe 201. (See column 9, lines 58-68).

As noted in Figure 2, there are three types of service responses 211 transmitted back to the requesting AMA probe 201 from the server computer 202. First, if the application program 203 on the server computer 202 properly responds to the service request, the AMA probe 201 will receive an indication of a successfully completed request i.e., a successful service response, from the server computer 202. Second, if the server computer 202 is unavailable to respond to the service request 210, the request will timeout after a predetermined period and the AMA probe 201 will record that the server computer was not available, and indicate this as an unsuccessful service response. Third, if the server computer 202 rejects the service request 210, the AMA probe will again record the transaction as an unsuccessful service response 211. (See column 10, lines 29-45). Whether it is successful or unsuccessful, the service response 211 from the application program 203 on the server computer 202 (including the determination of a no-response time-out) is received at the AMA probe 201, which then records the results of the

transaction in a database repository 204. (See column 10, lines 52-57).

Reps does not provide any teaching of a computer security threat procedure comprising one or more steps for one of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat and executing a computer security threat procedure. Instead of a computer security threat, *Reps* is primarily concerned with the level of service and performance of an application program 203 residing on a server 202. *Reps* merely records the response 211 from the application program 203, whether the service request 210 was successful or unsuccessful. *Reps* is not concerned with why a service request 210 may not have been successful.

In the Office Action dated March 20, 2007, the Examiner admitted that *Reps* also does not teach the claimed monitoring, problem determination, and remediation steps for attacks and automatically selecting a computer to execute the computer security step. The Examiner cited *Shostack* as allegedly disclosing these features. Therefore, Appellant submits that *Reps* does not anticipate or render obvious independent Claim 51.

Applicant further submits that *Reps* and *Shostack*, either alone or in combination, do not anticipate or render obvious independent Claim 51. *Reps* and *Shostack* do not teach accessing a table comprising computer locations, Internet address ranges associated with the computer locations, and computer security threat procedure associated with the computer locations, the computer security threat procedure comprising one or more steps for one of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat, and the computer locations identifying devices that are able to perform the computer security threat procedure associated with the computer security step information, as recited in independent Claim 51.

In the Office Action dated March 20, 2007, the Examiner's cited Column 5, lines 46-48 and Column 11, lines 51-52 of *Reps*, reproduced below, as allegedly disclosing some aspects of accessing a table comprising computer locations for one of investigating and responding to one of suspicious computer activity.

> "In an embodiment of the invention these parameters may include such information as the name of the application program, the address of the server system..." Reps reference, column 5, lines

46-48.

> "[T]he probe configuration information 302 will include…the network address of the target server and the type of application on the target server to be monitored…." Reps reference, column 11, lines 48-53.

However, these passages only discuss storing location information to access the application server of *Reps*. The application server of *Reps* is not a computer location that is able to perform computer security steps associated with the computer security step information for one of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat, as recited in independent Claim 51.

Furthermore, as noted above with respect to independent Claim 1, neither *Reps* nor *Shostack* provides any teaching of storing a permanent record comprising the executed computer security threat procedure and result information, and corresponding date and time stamps, as recited in independent Claim 51.

Therefore, Appellant submits that the cited documents, including *Shostack* and *Reps*, either alone or in combination, do not anticipate or render obvious independent Claim 42. Accordingly, reconsideration and withdrawal of the rejection of Claim 42 are respectfully requested.

Independent Claim 56

In the Office Action dated March 20, 2007, the Examiner rejected independent Claim 56 as allegedly being obvious in view of *Shostack* and *Trcka*. Appellant respectfully traverses this rejection. In particular, Appellant respectfully submits that the Examiner has not established a *prima facie* case of obviousness with respect to independent Claim 1 because the cited documents, including *Shostack* and *Trcka*, fail to teach or suggest at least the combination of the features of: (1) receiving computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat; (2) classifying the computer security incident information; (3) displaying one or more tools for one of investigating and responding to computer security incident information; (4) automatically suggesting one or more tools based on a classification of the computer security incident information; (5) receiving a selection of a suggested tool; (6) in response to a selection of a tool, forwarding data for execution of the tool; and (7) forwarding data for storing a permanent record comprising computer security incident information, executed tool information, and corresponding date and time stamps.

In the Office Action dated March 20, 2007, the Examiner admitted that *Shostack* does not teach the claimed feature of a date and time stamp. Therefore, Appellant submits that *Shostack* does not anticipate or render obvious independent Claim 56. Applicant further submits that *Shostack* and *Trcka*, either alone or in combination, do not anticipate or render obvious independent Claim 56. As noted above with respect to independent Claim 1. As noted above with respect to independent Claim 1, neither *Shostack* nor *Trcka* disclose, teach, or suggest at least the features of: (1) displaying one or more computer security threat investigation procedures and response procedures; and (2) receiving a selection of a computer security threat investigation procedure. Nor do *Shostack* or *Trcka* disclose, teach, or suggest the corresponding steps of: (1) displaying one or more tools for investigating or responding to computer security incident information; (2) automatically suggesting one or more tools based on a classification of the computer security incident information; (3) receiving a selection of a suggested tool; (4) forwarding data for execution of a selected tool; or (5) forwarding data for storing a permanent record comprising computer security incident information, executed tool information, corresponding date and time stamps, as recited in independent Claim 56.

Therefore, Appellant submits that the cited documents, including *Shostack* and *Trcka*, either alone or in combination, do not anticipate or render obvious independent Claim 56. Accordingly, reconsideration and withdrawal of the rejection of Claim 56 are respectfully requested.

Dependent Claims 2-9, 11-41, 43-50, 52-55, and 57-65

Appellant respectfully submits that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited documents. Appellant also respectfully submits that the recitations of these dependent claims are of patentable significance.

In view of the foregoing, Appellant respectfully requests that the Examiner withdraw the pending rejections of dependent Claims 2-9, 11-41, 43-50, 52-55, and 57-65.

Conclusion

In view of the arguments presented herein, Appellant respectfully requests that the final rejection in this matter be vacated, and that this application be returned to the Examiner with instructions to enter a notice of allowance.

Respectfully submitted,
/SPW/
Steven P. Wigmore
Reg. No. 40,447

KING & SPALDING LLP
1180 Peachtree Street
34th Floor
Atlanta, GA 30309
(404) 572-4600 (Telephone)
(404) 572-5134 (Facsimile)

APPENDIX 1

CLAIMS APPENDIX

1. (Previously Presented) A method for automatically creating a record for one or more computer security incidents and reactions thereto, comprising the steps of:

recording computer security incident information with at least one of a date and time stamp, the computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat;

classifying the computer security incident information;

automatically suggesting one or more computer security threat procedures based on a classification of the computer security incident information;

displaying the one or more suggested computer security threat procedures, each computer security threat procedure comprising one or more steps for one of investigating and responding to the computer security incident information;

receiving a selection of a suggested computer security threat procedure from a user, the selection comprising one or more steps of the selected computer security threat procedure;

executing the selected one or more steps of the computer security threat procedure;

in response to executing the one or more steps of the selected computer security threat procedure, recording executed computer security threat procedure information and results of the executed one or more steps of the computer security threat procedure with at least one of a date and time stamp; and

outputting a record comprising the computer security incident information, executed computer security threat procedure information, results of one or more steps of the executed computer security threat procedure, an identity of the user who selected the computer security threat procedure, and at least one of a corresponding date stamp and time stamp.

2. (Original) The method of Claim 1, wherein the record comprises an unmodifiable, permanent database.

3. (Previously Presented) The method of Claim 1, further comprising the step of recording the results of the executed computer security threat procedure with a digital signature to enable detection of any modification of the recorded results, whereby integrity of the recorded results can be monitored.

4. (Previously Presented) The method of Claim 1, further comprising the step of extracting information from the results of an executed computer security threat procedure.

5. (Previously Presented) The method of Claim 4, further comprising the step of describing a computer security incident with said extraction information.

6. (Previously Presented) The method of Claim 1, further comprising the step of displaying information for a particular computer security incident to more than one user.

7. (Original) The method of Claim 1, further comprising the step of prepopulating fields of a record of a first program module from a second program module.

8. (Previously Presented) The method of Claim 1, further comprising the steps of:

receiving computer security incident information from a first program module;

processing the computer security incident information with a second program module; and

forwarding the processed computer security incident information from the second program module to a third program module.

9. (Previously Presented) The method of Claim 1, wherein the step of receiving a selection of a computer security threat procedure comprises automatically selecting a computer security threat procedure with a program module.

10. (Cancelled)

11. (Original) The method of Claim 1, wherein each step is performed automatically by a program module.

12. (Original) The method of Claim 1, wherein some of the steps are performed automatically by a program module.

13. (Original) The method of Claim 1, further comprising the step of displaying reports comprising one or more computer security incidents.

14. (Previously Presented) The method of Claim 1, wherein the results of an executed computer security threat procedure comprise at least one of text, numbers, images, or formatted documents.

15. (Previously Presented) The method of Claim 1, further comprising the step of predicting future actions of a source of a computer security incident.

16. (Previously Presented) The method of Claim 1, further comprising the step of identifying the source of a computer security incident.

17. (Previously Presented) The method of Claim 1, further comprising the step of sorting decoy or false computer security incidents from actual computer security incidents.

18. (Previously Presented) The method of Claim 1, further comprising the step linking a first computer security threat procedure to a second computer security threat procedure.

19. (Original) The method of Claim 1, further comprising the step of determining the authorization level of a user.

20. (Previously Presented) The method of Claim 1, wherein the step providing data to enable display of a computer security threat procedure further comprises the step of providing data for enabling display of one or more steps of a computer security threat procedure.

21. (Previously Presented) The method of Claim 1, further comprising the steps of:

providing data to enable display of a computer security threat response procedure;

executing the computer security threat response procedure; and

in response to executing the response computer security threat procedure, recording executed computer security threat response procedure information and results of the executed computer security threat response procedure with at least one of a date and time stamp.

22. (Previously Presented) The method of Claim 1, further comprising the steps of:

providing data to enable display of a computer security threat investigation procedure;

executing the computer security threat investigation procedure; and

in response to executing the computer security threat investigation procedure, recording executed computer security threat investigation procedure information and results of the executed computer security threat investigation procedure with at least one of a date and time stamp.

23. (Previously Presented) The method of Claim 21, wherein the step of providing data to enable display of the computer security threat response procedure further comprises the step of providing data to enable display of one or more steps of the computer security threat response procedure.

24. (Previously Presented) The method of Claim 1, further comprising the step of providing data to enable display of results of the executed computer security threat procedure.

25. (Previously Presented) The method of Claim 23, further comprising the step of providing data to enable display of results of the executed computer security threat procedure.

[The remainder of this page has been intentionally left blank.]

26. (Previously Presented) The method of Claim 1, further comprising the steps of:

identifying an appropriate computer to execute a step in the computer security threat investigation procedure; and

identifying an appropriate computer to execute a step in the computer security threat response procedure.

27. (Original) The method of Claim 26, further comprising the steps of:

accessing a table comprising computer locations and step information;

comparing a step to be executed with computer locations listed in the table;

determining a match exists between the step to be executed and the computer locations; and

if one or more matches exist, displaying the matching information or automatically selecting an appropriate location.

28. (Previously Presented) The method of Claim 27, wherein the table further comprises Internet address ranges, the method further comprising the step of comparing an Internet address of a source of a computer security incident with the Internet address ranges of the table.

29. (Original) The method of Claim 27, further comprising the step of providing data to enable display of an appropriate substitute computer location if a match does not exist.

30. (Previously Presented) The method of Claim 27, further comprising the step of identifying an appropriate computer to execute a step in either an investigation or a computer security threat response procedure, wherein the computer is strategically located relative to a source of a computer security incident.

31. (Previously Presented) The method of Claim 1, wherein each computer security threat procedure comprises one or more steps, the method further comprising the step of executing one or more program modules in response to a selection of a computer security threat procedure.

32. (Original) The method of Claim 31, wherein the one or more program modules comprise one or more software application programs that can operate as stand alone programs.

33. (Original) The method of Claim 31, wherein at least one program module comprises an off-the-shelf software application program.

34. (Previously Presented) The method of Claim 1, wherein the computer security incident information comprises predefined attributes.

35. (Original) The method of Claim 34, wherein the predefined attributes comprise any one of a computer incident severity level, a computer incident category, a computer incident scope value, a computer incident status value, an attacker internet protocol (IP) address value, an attacker ISP name, an attacker country, an external attacker status value, an incident type vale, a vulnerabilities level, an entry point value, an attack profile value, a target networks value, a target firewalls value, a target hosts value, a target services value, a target accounts value, and a damage type value.

36. (Previously Presented) The method of Claim 1, wherein the computer security incident information comprises attributes that are at least one of viable and computer-generated.

37. (Previously Presented) The method of Claim 35, further comprising the step of determining whether a computer security incident comprises an actual breach in security based upon value of its attributes.

38. (Previously Presented) The method of Claim 1, further comprising the steps of:

receiving a selection for a step of a computer security threat procedure; and

generating a pre-execution warning prior to the selection of a step.

[The remainder of this page has been intentionally left blank.]

39. (Previously Presented) The method of Claim 1, further comprising the steps of:

receiving a selection for a step of a computer security threat procedure;

executing the selected step; and

suggesting an appropriate subsequent step in the computer security threat procedure.

40. (Previously Presented) The method of Claim 1, wherein each step is performed automatically in response to a detected computer security incident.

41. (Original) The method of Claim 1, further comprising the steps of:

providing data to enable display of a plurality of computer tools in a non-procedural manner;

receiving a selection for a computer tool; and

executing the selected computer tool.

[The remainder of this page has been intentionally left blank.]

42. (Previously Presented) A method for organizing and recording reactions to one or more computer security incidents, comprising the steps of:

classifying the computer security incident information;

automatically suggesting one or more computer security threat investigation procedures based on a classification of the computer security incident information;

displaying the one or more computer security threat investigation procedures for investigating one of suspicious computer activity that occur prior to a computer security threat and an actual computer security threat;

displaying one or more computer security threat response procedures for responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat;

in response to a selection of a computer security threat investigation procedure, displaying one or more corresponding investigation steps;

in response to a selection of a computer security threat response procedure, displaying one or more corresponding response steps;

receiving a selection of one or more investigation steps and one or more corresponding response steps;

storing a permanent record comprising computer security incident information, executed investigation step and result information, executed response step and result information, and corresponding date and time stamps.

43. (Previously Presented) The method of Claim 42, further comprising the step of recording executed investigation step information and results of the executed investigation step with at least one of a date and time stamp in response to a selection of a step of computer security threat investigation procedure.

44. (Previously Presented) The method of Claim 42, further comprising the step of recording executed response step information and results of the executed response step with at least one of a date and time stamp in response to a selection of a step of a computer security threat response procedure.

45. (Previously Presented) The method of Claim 42, further comprising the steps of:

providing data to enable display of a plurality of computer security threat procedures;

in response to receiving a selection of a computer security threat procedure, displaying a plurality of steps;

obtaining modification information for the selected computer security threat procedure; and

storing the modification information.

46. (Previously Presented) The method of Claim 42, further comprising the step of at least one of adding or deleting a step in a computer security threat procedure.

47. (Previously Presented) The method of Claim 42, further comprising the steps of:

providing data to enable display of a plurality of steps of a computer security threat procedure;

in response to selection of a step, providing data to enable display of detailed information fields related to the selected step;

obtaining modification information for the selected step; and

storing the modification information.

48. (Previously Presented) The method of Claim 42, further comprising the step of at least one of adding, deleting, or modifying a step in a computer security threat procedure.

49. (Original) The method of Claim 42, further comprising the steps of:

obtaining computer security incident search information; and

providing data to enable display of one or more computer security incidents matching the computer security incident search information.

[The remainder of this page has been intentionally left blank.]

50. (Original) The method of Claim 42, further comprising the steps of:

tracking multiple computer security incidents; and

storing information for each computer security in accordance with at least one of date and time stamp.

[The remainder of this page has been intentionally left blank.]

51. (Previously Presented) A method for selecting a computer that is strategically located relative to a source of a computer security incident, comprising the steps of:

accessing a table comprising computer locations, Internet address ranges associated with the computer locations, and computer security threat procedure associated with the computer locations, the computer security threat procedure comprising one or more steps for one of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat, the computer locations identifying devices that are able to perform the computer security threat procedure;

comparing a computer security threat procedure to be executed and a target Internet address with computer locations and Internet address ranges listed in the table;

determining if a match exists between an Internet address of a computer security incident and the Internet address ranges listed in the table;

automatically selecting a computer to execute the computer security threat procedure based upon the matching step, wherein the computer has a location and is capable of interacting with the Internet address of the computer security incident; and

storing a permanent record comprising the executed computer security threat procedure and result information, and corresponding date and time stamps.

52. (Original) The method of Claim 51, further comprising the step of:

if one or more matches exist, providing data to enable display of the matching information;

if a match does not exist, providing data to enable display of one or more appropriate substitute computer locations or automatically selecting an appropriate location.

53. (Previously Presented) The method of Claim 51, wherein the computer security threat procedure comprises a portion of a computer security threat response procedure, wherein the computer is strategically located relative to a source of a computer security incident.

54. (Previously Presented) The method of Claim 51, wherein the computer security threat procedure comprises a portion of a computer security threat investigation procedure, wherein the

computer is strategically located relative to a source of a computer security incident.

55. (Previously Presented) The method of Claim 51, wherein each computer security threat procedure step to be executed in a computer security threat procedure comprises one or more off-the-shelf security application programs.

[The remainder of this page has been intentionally left blank.]

56. (Previously Presented) A method for generating a permanent record of one of more computer security incidents and reactions thereto, comprising the steps of:

receiving computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat;

classifying the computer security incident information;

displaying one or more tools for one of investigating and responding to computer security incident information;

automatically suggesting one or more tools based on a classification of the computer security incident information;

receiving a selection of a suggested tool;

in response to a selection of a tool, forwarding data for execution of the tool; and

forwarding data for storing a permanent record comprising computer security incident information, executed tool information, and corresponding date and time stamps.

57. (Original) The method of Claim 56, further comprising the step of displaying the tools as icons on a computer display.

58. (Original) The method of Claim 56, further comprising the step of displaying a plurality of tools that are selectable from a menu.

59. (Original) The method of Claim 31, further comprising the step of installing the one or more program modules within a single program on a server.

60. (Original) The method of Claim 31, further comprising the step of installing the one or more program modules on a single server.

61. (Original) The method of Claim 31, further comprising the step of installing the one or more program modules on a computer that is a target of a computer incident.

62. (Original) The method of Claim 31, further comprising the step of installing the one or more computer modules on both a computer that is a target of a computer incident and a server.

63. (Original) The method of Claim 27, wherein the table further comprises Internet address ranges, the method further comprising the step of comparing an Internet address of a computer subject to an attack or security breach with the Internet address ranges of the table.

64. (Previously Presented) The method of Claim 27, wherein the table further comprises Internet address ranges, the method further comprising the step of comparing Internet address of a witness to a computer security incident with the Internet address ranges of the table.

65. (Previously Presented) The method of Claim 27, wherein the table further comprises Internet address ranges, the method further comprising the step of comparing an Internet address of an accomplice to a computer security incident with the Internet address ranges of the table.

[The remainder of this page has been intentionally left blank.]

APPENDIX 2

EVIDENCE APPENDIX

None.

APPENDIX 3

RELATED PROCEEDINGS APPENDIX

None.